Copy for Administrative Patent Judge

#5C

Patent 2/5/01, MW.

Attorney's Docket No. 032406-002

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Karl L. GINTER, et al.	)	Group Art Unit: 2171
	)	
Application No.: 09/411,205	)	Examiner: Von Buhr, M.
	)	
Filed: October 4, 1999	)	
	)	
For: SYSTEMS AND METHODS FOR SECURE TRANSACTION MANAGEMENT AND ELECTRONIC RIGHTS PROTECTION	)	

AMENDMENT AND REQUEST FOR INTERFERENCE

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In response to the Office Action dated December 19, 2000, please amend the above-identified application as follows:

IN THE SPECIFICATION:

On page 1, before the heading "Field(s) of the Invention(s)," insert the following paragraph:

--This application is a continuation of Application No. 09/208,017 filed December 9, 1999, which is a continuation of Application No. 08/388,107 filed February 13, 1995, now abandoned.--

IN THE CLAIMS:

Please cancel claims 1-90 of the application as originally filed and add new claims 91-148 as follows:

--91. A method for managing a data object so as to comply with control conditions for usage of the data object, comprising the steps of:

storing the data object in a memory device, where it is accessible by means of a data object provider's data processor;

providing a variable number of control conditions for usage of the data object;

creating, by said data processor, a general set of control data for the data object based on said variable number of control conditions for usage, said general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with said variable number of control conditions,

storing said general set of control data in a memory device, where it is accessible by said data processor;

concatenating the general set of control data with a copy of the data object; and

encrypting at least the copy of the data object and said one or more usage control elements to create a secure data package which is ready for transfer to a user.

92. A method as set forth in claim 91, wherein the step of encrypting comprises encrypting the data object and the general set of control data.

93. A method as set forth in claim 91, wherein the step of creating control data comprises creating an identifier which uniquely identifies the general set of control data.

94. A method as set forth in claim 91, wherein the step of creating a general set of control data comprises creating a security control element which identifies a security process to be applied before usage of the data object is allowed.

95. A method as set forth in claim 91, wherein the step of creating a general set of control data comprises creating a format control element which identifies the format of the control data.

96. A method as set forth in claim 91, further comprising the steps of receiving in said data processor a request for authorization for usage by a user; comparing the usage for which authorization is requested with said one or more usage control elements of the general set of control data and granting the authorization if the usage for which authorization is requested complies with the usages defined by said one or more usage control elements.

97. A method as set forth in claim 96, further comprising the step of securing payment for the requested authorization for usage before granting the authorization.

98. A method as set forth in claim 91, comprising the further steps of:

receiving the data package in a user's data processor;

storing the data package in a memory device where it is accessible by means of the user's data processor;

decrypting said one or more usage control elements;

checking, in response to a request by the user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the general set of control data;

decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the general set of control data, the data object and enabling the requested usage, otherwise disabling it.

99. A method as set forth in claim 98, comprising the further steps of reconcatenating, after the usage of the data object, the data object and the one or more usage control elements, reencrypting at least the data object and the one or more usage control elements, and storing the thus-repackaged data package in the memory of the user's data processor.

100. A method for controlling the usage by a user of a data object so as to comply with control conditions for usage of the data object, comprising the steps of:

providing a variable number of control conditions for usage of the data object;

storing a data package in a memory device, where it is accessible by means of a data processor of the user, said data package comprising the data object and control data, which comprises at least one usage control element defining a usage of the data object which complies with the variable number of control conditions, the data object and said at least one usage control element being encrypted;

receiving a request by the user for usage of the data object;

decrypting the control data;

checking, in response to the request by the user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the control data; and

decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the control data, the data object and enabling the requested usage, otherwise disabling it.

101. A method as set forth in claim 100, wherein the usage control element is updated after the at least one usage of the data object.

102. A method as set forth in claim 100, wherein said control data comprises an indication of the number of times the user is authorized to use the data object in accordance with said at least one usage control element;

wherein the requested usage of the data object is only enabled when said number of times is one or more; and

wherein said number of times is decremented by one when the requested usage is enabled.

103. A method as set forth in claim 100, wherein the control data comprise a security control element, and further comprising the step of carrying out, before each usage of the data object, a security procedure defined in the security control element.

104. A method as set forth in claim 100, wherein the step of checking whether the requested usage complies with the usage defined by the at least one usage control element comprises the step of checking that the user's data processor is capable of carrying out a security procedure specified in a security control element of the at least one usage control element, and if not, disabling the usage.

105. A method as set forth in claim 100, comprising the further steps of reconcatenating, after the usage of the data object, the data object and the one or more usage control elements, reencrypting at least the data object and the one or more usage control elements, and storing the thus-repackaged data package in the memory of the user's data processor.

106. A system for managing a data object so as to comply with control conditions for usage of the data object, comprising means for providing a variable number of control conditions;

first means in the data object provider's data processor for creating a general set of control data for the data object based on the variable number of control conditions for usage, said general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the variable number of control conditions;

storing means, which are accessible by means of said data processor, for storing the data object and the general set of control data;

concatenating means for concatenating the general set of control data with a copy of the data object; and

encrypting means for encrypting the copy of the data object and at least said one or more usage control elements to create a secure data package, which is ready for transfer to a user.

107. A system as set forth in claim 106, wherein the general set of control data comprises a control data element which defines the right to further distribution of the data object by the user.

108. A system for controlling the usage by a user of a data object so as to comply with control conditions for usage of the data object, comprising:

means for providing variable number of control conditions;

storing means for storing a data package which comprises a data object and a control data comprising at least one usage control element defying a usage of the data object which complies with the variable number of control conditions;

means for decrypting the at least one usage control element and the data object;

checking means for checking whether a usage requested by the user complies with the usage defined by said at least one usage control element;

enabling means for enabling the usage requested by the user when the usage complies with the usage defined by said at least one usage control element; and

disabling means for disabling the usage requested by the user when the usage does not comply with the usage defined by said at least one usage control element.

109. A system as set forth in claim 108, further comprising means for repackaging the data object after usage thereof.

110. A method for controlling the usage by a user of data objects so as to comply with predetermined conditions for usage of the data objects, comprising the steps of:

storing at least two data packages in a memory device, where they are accessible by a data processor of the user, each said data package comprising a data object and a user set of control data, which comprises at least one usage control element defining a usage of the data object which complies with the predetermined conditions, the data object and said at least one usage control elements being encrypted;

decrypting the usage control elements of the user sets of control data;

examining the usage control elements of said at least two data packages to find a match;

using, in response to the finding of a match, the data processor to carry out an action, which is specified in the user sets of control data.

111. A method as set forth in claim 110, comprising the further steps of updating the at least one usage control element of each data package, concatenating after the usage of the data objects, each of the data objects and its at least one usage control element, reencrypting each of the concatenated data objects and its at least one usage control element and transferring the repackaged data objects to their creators.

112. A method for managing a data object so as to comply with predetermined conditions for usage of the data object, comprising the steps of:

storing the data object in a memory device, where it is accessible by means of a data object provider's data processor;

providing control conditions for usage of the data object;

creating, by said data processor, a general set of control data for the data object based on said control conditions for usage, said general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with said control conditions;

storing said general set of control data in a memory device, where it is accessible by said data processor;

concatenating the general set of control data with a copy of the data object;

encrypting at least the copy of the data object and said one or more usage control elements to create a secure data package which is ready for transfer to a user;

creating, in response to a request for authorization for usage of the data object by a user, a user set of control data, which comprises at least a subset of the general set of control data, including at least one of said usage control elements;

using the user set of control data instead of the general set of control data in said concatenating step;

using the at least one or more usage control element of the user set of control data instead of the one or more usage control elements of the general set of control data in the encrypting step; and

checking, before allowing transfer of the data package to the user, that said request for authorization for usage of the data object has been granted.

113. A method as set forth in claim 112, wherein the data object is composed of at least two constituent data objects and wherein the user set of control data, in response to a request for authorization for usage of one of said constituent data objects by a user, is created only for that constituent data object and concatenated only with a copy of that constituent data object.

114. A method as set forth in claim 112, wherein the data provider's data processor is connected to a data network and the request for authorization is received from a data processor of the user, which is also connected to the data network, further comprising the step of transferring the data package through the data network to the user's data processor.

115. A method as set forth in claim 112, wherein the data object is a composite data object including at least two constituent data objects and wherein the step of creating a general set of control data comprises the step of creating a respective general set of control data for each of the constituent data objects and the composite data object and wherein the step of creating a user set of control data comprises the step of creating a respective user set of control data for each of the constituent data objects and the composite data object.

116. A method as defined in claim 112, comprising the further step of storing a copy of the user set of control data in the data object provider's processor.

117. A method as defined in claim 112, comprising the further steps of:

receiving the data package in a user's data processor;

storing the data package in a memory device where it is accessible by means of the user's data processor;

decrypting the at least one usage control element of the user set of control data;

checking, in response to a request by the user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the user set of control data; and

decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the user set of control data, the data object and enabling the requested usage, otherwise disabling it.

118. A method as set forth in claim 112, further comprising:

receiving the data package in a user's data processor;

storing the data package in a memory device where it is accessible by means of the user's data processor;

decrypting the at least one usage control element of the user set of control data;

checking, in response to a request by the user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the user set of control data;

decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the user set of control data, the data object and enabling the requested usage, otherwise disabling it; and

reconcatenating, after the usage of the data object, the data object and the one or more usage control elements of the user set of control data, and reencrypting at least the data object and the one or more usage of the user set of control data.

119. A system for managing a data object so as to comply with control conditions for usage of the data object, comprising:

first means in the data object provider's data processor for creating a general set of control data for the data object based on the predetermined conditions for usage, said general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the predetermined conditions;

storing means, which are accessible by means of said data processor, for storing the data object and the general set of control data;

concatenating means for concatenating the general set of control data with a copy of the data object;

encrypting means for encrypting the copy of the data object and at least said one or more usage control elements to create a secure data package, which is ready for transfer to a user;

second means in said data processor for creating, in response to a request for authorization for usage of the data object by a user, a user set of control data, which comprises at least a subset of the general set of control data, which subset comprises at least one of said usage control elements;

using the user set of control data instead of the general set of control data in the storing means;

using the user set of control data instead of the general set of control data in the concatenating means;

using the user set of control data instead of the general set of control data in the encrypting means; and

checking means in said data processor for checking that said request for authorization for usage of the data object has been granted before allowing transfer of the data package to the user.

120. A method for managing an object so as to comply with control conditions for usage of the object, comprising the steps of:

storing the object in a storage device, where it is accessible by means of an object provider's electronic appliance;

providing a variable number of control conditions for usage of the object;

creating, by said electronic appliance, a general set of control data for the object based on said variable number of control conditions for usage, said general set of control data comprising at least one or more usage control elements defining usages of the object which comply with said variable number of control conditions,

storing said general set of control data in a storage device, where it is accessible by said electronic appliance;

containerizing the general set of control data with a copy of the object; and

encrypting at least the copy of the object and said one or more usage control elements to create a secure container which is ready for transfer to a user.

121. A method as set forth in claim 120, wherein the step of encrypting comprises encrypting the object and the general set of control data.

122. A method as set forth in claim 120, wherein the step of creating control data comprises creating an identifier which uniquely identifies the general set of control data.

123. A method as set forth in claim 120, wherein the step of creating a general set of control data comprises creating a security control element which identifies a security process to be applied before usage of the object is allowed.

124. A method as set forth in claim 120, wherein the step of creating a general set of control data comprises creating a format control element which identifies the format of the control data.

125. A method as set forth in claim 120, further comprising the steps of receiving in said electronic appliance a request for authorization for usage by a user; comparing the usage for which authorization is requested with said one or more usage control elements of the general set of control data and granting the authorization if the usage for which authorization is requested complies with the usages defined by said one or more usage control elements.

126. A method as set forth in claim 125, further comprising the step of securing payment for the requested authorization for usage before granting the authorization.

127. A method as set forth in claim 120, comprising the further steps of:

receiving the container in a user's electronic appliance;

storing the container in a storage device where it is accessible by means of the user's electronic appliance;

decrypting said one or more usage control elements;

checking, in response to a request by the user for usage of the object, whether the requested usage complies with the usage defined by the at least one usage control element of the general set of control data;

decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the general set of control data, the object and enabling the requested usage, otherwise disabling it.

128. A method as set forth in claim 127, comprising the further steps of recontainerizing, after the usage of the object, the object and the one or more usage control elements, reencrypting at least the object and the one or more usage control elements, and storing the thus-recontainerized container in the storage of the user's electronic appliance.

129. A method for controlling the usage by a user of an object so as to comply with control conditions for usage of the object, comprising the steps of:

providing a variable number of control conditions for usage of the object;

storing a container in a storage device, where it is accessible by means of an electronic appliance of the user, said container comprising the object and control data, which comprises at least one usage control element defining a usage of the object which complies with the variable number of control conditions, the object and said at least one usage control element being encrypted;

receiving a request by the user for usage of the object;

decrypting the control data;

checking, in response to the request by the user for usage of the object, whether the requested usage complies with the usage defined by the at least one usage control element of the control data; and

decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the control data, the object and enabling the requested usage, otherwise disabling it.

130. A method as set forth in claim 129, wherein the usage control element is updated after the at least one usage of the object.

131. A method as set forth in claim 129, wherein said control data comprises an indication of the number of times the user is authorized to use the object in accordance with said at least one usage control element;

wherein the requested usage of the object is only enabled when said number of times is one or more; and

wherein said number of times is decremented by one when the requested usage is enabled.

132. A method as set forth in claim 129, wherein the control data comprise a security control element, and further comprising the step of carrying out, before each usage of the object, a security procedure defined in the security control element.

133. A method as set forth in claim 129, wherein the step of checking whether the requested usage complies with the usage defined by the at least one usage control element comprises the step of checking that the user's electronic appliance is capable of carrying out a security procedure specified in a security control element of the at least one usage control element, and if not, disabling the usage.

134. A method as set forth in claim 129, comprising the further steps of recontainerizing, after the usage of the object, the object and the one or more usage control elements, reencrypting at least the object and the one or more usage control elements, and storing the thus-recontainerized container in the storage of the user's electronic appliance.

135. A system for managing an object so as to comply with control conditions for usage of the object, comprising means for providing a variable number of control conditions;

first means in the object provider's electronic appliance for creating a general set of control data for the object based on the variable number of control conditions for usage, said general set of control data comprising at least one or more usage control

elements defining usage of the object which comply with the variable number of control conditions;

storing means for storing a container which comprises the object and a control data in combination with the general set of control data;

containerizing means for containerizing the general set of control data with a copy of the object; and

encrypting means for encrypting the copy of the object and at least said one or more usage control elements of the object to be contained in the container which is ready for transfer to the user.--

---

136. A system as set forth in claim 135, wherein the general set of control data comprises a control data element which defines the right to further distribution of the object by the user.

137. A system for controlling the usage by a user of an object so as to comply with control conditions for usage of the object, comprising:

means for providing variable number of control conditions;

storing means for storing a container which comprises an object and a control data comprising at least one usage control element defying a usage of the object which complies with the variable number of control conditions;

means for decrypting the at least one usage control element and the object;

recontainerizing, after the usage of the object, the object and the one or more checking means for checking whether a usage requested by the user complies

usage control elements of the user set of control data, and reencrypting at least the object with the usage defined by said at least one usage control element;

and the one or more usage of the user set of control data.
enabling means for enabling the usage requested by the user when the usage

complies with the usage defined by said at least one usage control element; and

148. A system for managing an object so as to comply with control conditions for disabling means for disabling the usage requested by the user when the usage

usage of the object, comprising:
does not comply with the usage defined by said at least one usage control element.

first means in the object provider's electronic appliance for creating a general

set of control data for the object based on the predetermined conditions for usage, said
138. A system as set forth in claim 137, further comprising means for

general set of control data comprising at least one or more usage control elements defining
recontainerizing the object after usage thereof.

usages of the object which comply with the predetermined conditions;

storing means, which are accessible by means of said electronic appliance, for
139. A method for controlling the usage by a user of objects so as to comply with

storing the object and the general set of control data;
predetermined conditions for usage of the objects, comprising the steps of:

containerizing means for containerizing the general set of control data with a
storing at least two containers in a storage device, where they are accessible

copy of the object;
by an electronic appliance of the user, each said container comprising an object and a user

encrypting means for encrypting the copy of the object and at least said one or
set of control data, which comprises at least one usage control element defining a usage of

more usage control elements to create a secure container, which is ready for transfer to a
the object which complies with the predetermined conditions, the object and said at least

user;
one usage control elements being encrypted;

second means in said electronic appliance for creating, in response to a request
decrypting the usage control elements of the user sets of control data;

for authorization for usage of the object by a user, a user set of control data, which
examining the usage control elements of said at least two containers to find a

comprises at least a subset of the general set of control data, which subset comprises at
match;

least one of said usage control elements;

checking, in response to a request by the user for usage of the object, whether the requested usage complies with the usage defined by the at least one usage control element of the user set of control data; and

decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the user set of control data, the object and enabling the requested usage, otherwise disabling it.

140. A method as set forth in claim 139, comprising the further steps of creating a container, containerizing after the usage of the object, each object and its at least one usage control element, reencrypting each of the contained objects and its at least one usage control element and transferring the containerized objects to their owners.

141. A method as set forth in claim 140, further comprising:

receiving the container in a user's electronic appliance;

storing the container in a storage device where it is accessible by means of the user's electronic appliance.

142. A method for managing an object so as to comply with predetermined conditions for usage of the object, comprising the steps of:

storing the object in a storage device, where it is accessible by means of an object provider's data processor;

providing control conditions for usage of the object;

creating, by said electronic appliance, a general set of control data for the object based on said control conditions for usage, said general set of control data comprising at least one or more usage control elements defining usages of the object which comply with said control conditions;

storing said general set of control data in a storage device, where it is accessible by said electronic appliance;

containerizing the general set of control data with a copy of the object;

comprising the step of transferring the container through the data network to the user's electronic appliance.

144. A method as set forth in claim 141, wherein the object is a composite object including at least one of said usage control elements, wherein the step of creating a general set of control data comprises the step of creating a respective general set of control data for each of the constituent objects and the composite object and wherein the step of creating a user set of control data comprises the step of creating a respective user set of control data for each of the constituent objects and the composite object.

145. A method as defined in claim 144, comprising the further step of storing a copy of the authorization for usage of the object has been granted.

146. A method as defined in claim 141, wherein the object is composed of at least two constituent objects and wherein the user set of control data, in response to a request for authorization for usage of one of said constituent objects by a user, is created only for that user's electronic appliance.

decrypting the at least one usage control element of the user set of control data; 143. A method as set forth in claim 141, wherein the data provider's electronic appliance is connected to a data network and the request for authorization is received from an electronic appliance of the user, which is also connected to the data network, further

comprising the step of transferring the container through the data network to the user's electronic appliance.

144. A method as set forth in claim 141, wherein the object is a composite object including at least two constituent objects and wherein the step of creating a general set of control data comprises the step of creating a respective general set of control data for each of the constituent objects and the composite object and wherein the step of creating a user set of control data comprises the step of creating a respective user set of control data for each of the constituent objects and the composite object.

145. A method as defined in claim 141, comprising the further step of storing a copy of the user set of control data in the object provider's processor.

146. A method as defined in claim 141, comprising the further steps of:

receiving the container in a user's electronic appliance;

storing the container in a storage device where it is accessible by means of the user's electronic appliance;

decrypting the at least one usage control element of the user set of control data;

checking, in response to a request by the user for usage of the object, whether the requested usage complies with the usage defined by the at least one usage control element of the user set of control data; and

decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the user set of control data, the object and enabling the requested usage, otherwise disabling it.

147. A method as set forth in claim 141, further comprising:

receiving the container in a user's electronic appliance;

storing the container in a storage device where it is accessible by means of the user's electronic appliance;

checking, before allowing transfer of the container to the user, that said request for authorization for usage of the object has been granted.

142. A method as set forth in claim 141, wherein the object is composed of at least two constituent objects and wherein the user set of control data, in response to a request for authorization for usage of one of said constituent objects by a user, is created only for that constituent object and contained only with a copy of that constituent object.

143. A method as set forth in claim 141, wherein the data provider's electronic appliance is connected to a data network and the request for authorization is received from an electronic appliance of the user, which is also connected to the data network, further

using, in response to the finding of a match, the electronic appliance to carry recontainerizing, after the usage of the object, the object and the one or more out an action, which is specified in the user sets of control data, usage control elements of the user set of control data, and reencrypting at least the object and the one or more usage of the user set of control data.

140. A method as set forth in claim 139, comprising the further steps of updating the at least one usage control element of each container, containerizing after the usage of

148. A system for managing an object so as to comply with control conditions for the objects, each of the objects and its at least one usage control element, reencrypting each usage of the object, comprising:

of the contained objects and its at least one usage control element and transferring the first means in the object provider's electronic appliance for creating a general recontainerized objects to their owners.
set of control data for the object based on the predetermined conditions for usage, said general set of control data comprising at least one or more usage control elements defining

141. A method for managing an object so as to comply with predetermined usages of the object which comply with the predetermined conditions; conditions for usage of the object, comprising the steps of:

storing means, which are accessible by means of said electronic appliance, for storing the object in a storage device, where it is accessible by means of an storing the object and the general set of control data;
object provider's data processor;

containerizing means for containerizing the general set of control data with a providing control conditions for usage of the object; copy of the object;

creating, by said electronic appliance, a general set of control data for the encrypting means for encrypting the copy of the object and at least said one or object based on said control conditions for usage, said general set of control data more usage control elements to create a secure container, which is ready for transfer to a comprising at least one or more usage control elements defining usages of the object which user;
comply with said control conditions;

second means in said electronic appliance for creating, in response to a request storing said general set of control data in a storage device, where it is for authorization for usage of the object by a user, a user set of control data, which accessible by said electronic appliance;
comprises at least a subset of the general set of control data, which subset comprises at containerizing the general set of control data with a copy of the object; least one of said usage control elements;

checking means for checking whether a usage requested by the user complies using the user set of control data instead of the general set of control data in the storing means, with the usage defined by said at least one usage control element;

enabling means for enabling the usage requested by the user when the usage complies using the user set of control data instead of the general set of control data in the containerizing means, with the usage defined by said at least one usage control element; and

disabling means for disabling the usage requested by the user when the usage does not comply using the user set of control data instead of the general set of control data in the encrypting means, and the usage defined by said at least one usage control element.

checking means in said electronic appliance for checking that said request for authorization for usage of the object has been granted before allowing transfer of the container to the user.

138. A system as set forth in claim 137, further comprising means for recontainerizing the object after usage thereof.

---

139. A method for controlling the usage by a user of objects so as to comply with predetermined conditions for usage of the objects, comprising the steps of:

storing at least two containers in a storage device, where they are accessible by an electronic appliance of the user, each said container comprising an object and a user set of control data, which comprises at least one usage control element defining a usage of the object which complies with the predetermined conditions, the object and said at least one usage control elements being encrypted;

decrypting the usage control elements of the user sets of control data;

examining the usage control elements of said at least two containers to find a match;